MEMORANDUM
RM-3898-PR
MARCH 1965

A NOTE ON THE SOLUTION OF POLYNOMIAL CONGRUENCES

Richard Bellman

PREPARED FOR:

UNITED STATES AIR FORCE PROJECT RAND

The RAND Corporation
SANTA MONICA • CALIFORNIA

MEMORANDUM
RM-3898-PR
MARCH 1965

A NOTE ON THE SOLUTION OF POLYNOMIAL CONGRUENCES

Richard Bellman

This research is sponsored by the United States Air Force under Project RAND—Contract No. AF 49(638)-700 monitored by the Directorate of Development Plans, Deputy Chief of Staff, Research and Development, Hq USAF. Views or conclusions contained in this Memorandum should not be interpreted as representing the official opinion or policy of the United States Air Force.

The RAND Corporation
1700 MAIN ST • SANTA MONICA • CALIFORNIA • 90406

PREFACE

Part of the Project RAND research program consists of basic supporting studies in mathematics. The present Memorandum makes a contribution to the theory of polynomial congruences.

SUMMARY

As is well known, the number of solutions of the congruence

(1) $$f(x) \equiv 0(p),$$

where $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$, can be expressed in the form

$$N = \frac{1}{p} \sum_{t,x} e^{2\pi i t f(x)/p},$$

where t and x run independently through the values $0, 1, 2, \ldots, p-1$. This result is an immediate consequence of the relation

$$\sum_t e^{2\pi i t y/p} = 0, \quad y \not\equiv 0(p),$$

$$= p, \quad y \equiv 0(p).$$

In this note we present an alternative expression for the number of solutions of (1).

CONTENTS

A NOTE ON THE SOLUTION OF POLYNOMIAL CONGRUENCES

1. INTRODUCTION

It is well known that the number of solutions of the congruence

$$(1.1) \qquad f(x) \equiv 0(p),$$

where $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$, can be expressed in the form

$$(1.2) \qquad N = \frac{1}{p} \sum_{t,x} e^{2\pi i t f(x)/p},$$

where t and x run independently through the values $0,1,2,\ldots,p-1$. This result is an immediate consequence of the relation

$$(1.3) \qquad \sum_{t} e^{2\pi i t y/p} = 0, \quad y \not\equiv 0(p),$$

$$= p, \quad y \equiv 0(p).$$

In this note we present an alternative expression for the number of solutions of (1.1).

2. AN EQUIVALENT VECTOR-MATRIX CONGRUENCE

The equation $f(x) = 0$ is readily seen to be the characteristic equation of the matrix

$$(2.1) \qquad A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & & \\ -a_n & -a_{n-1} & -a_{n-2} & \cdots & -a_1 \end{pmatrix};$$

see [1], p. 225.

Using arguments completely analogous to that for the complex field, we see that a necessary and sufficient condition for a nontrivial solution of the vector-matrix congruence

$$(2.2) \qquad Ax \equiv \lambda x (p),$$

where x is now the n-dimensional column vector with components $x_1, x_2, \ldots, x_n$, and λ is a scalar, is that

$$(2.3) \qquad f(\lambda) \equiv 0 (p).$$

Each root of (2.3) generates a ray of solutions kx, where $k = 1, 2, \ldots, p-1$.

3. MULTIDIMENSIONAL EXPONENTIAL SUM

Let t be an n-dimensional vector with components $t_1, t_2, \ldots, t_n$, and let (t,x) denote, as usual, the vector inner product. We can then write, as the number of nontrivial solutions of (2.2),

$$(3.1)\qquad \sum_{t}\sum_{\lambda}\sum_{x}{}' e^{\frac{2\pi i}{p}(t,Ax-\lambda x)},$$

where (u,v) denotes the usual inner product and the prime denotes the fact that $x = 0$ is omitted in the summation.

Since each solution of $f(\lambda) = 0$ generates $p - 1$ solutions of (2.2), we have

$$(3.2)\qquad N = \frac{1}{p^n(p-1)} \sum_{t}\sum_{\lambda}\sum_{x}{}' e^{\frac{2\pi i}{p}(t,Ax-\lambda x)}.$$

We can eliminate the prime by writing

$$(3.3)\qquad N = \frac{1}{p^n(p-1)} \sum_{t,\lambda,x} e^{\frac{2\pi i}{p}(t,Ax-\lambda x)} - \frac{p}{p-1}.$$

Summing over the scalar λ first, we have finally

$$(3.4)\qquad N = \frac{1}{p^{n-1}(p-1)} \sum_{(t,x)=0(p)} e^{2\pi i(t,Ax)/p} - \frac{p}{p-1}.$$

If A is symmetric, we write $t = u + v$, $x = u - v$, and obtain

$$(3.5)\qquad N = \frac{1}{p^{n-1}(p-1)} \sum_{(u,u)=(v,v)(p)} e^{\frac{2\pi i}{p}[(u,Au)-(v,Av)]} - \frac{1}{p-1}.$$

This, in turn, may be written

$$(3.6) \qquad N = \frac{1}{p^{(n-1)}(p-1)} \sum_{k} \left| \sum_{(u,u) \equiv k(p)} e^{\frac{2\pi i}{p}(u,Au)} \right|^2 - \frac{p}{p-1},$$

an interesting formula.

4. EXAMPLE

Consider the congruence

$$(4.1) \qquad \lambda^3 + a \equiv 0(p).$$

The corresponding matrix is

$$(4.2) \qquad A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -a & 0 & 0 \end{pmatrix}.$$

Hence, the number of solutions of (4.1) is given by

$$(4.3) \qquad N = \frac{1}{p^2(p-1)} \sum_{S} e^{\frac{2\pi i}{p}(t_1x_2+t_2x_3-at_3x_1)} - \frac{p}{p-1},$$

where the set of values S is determined by
$t_1x_1 + t_2x_2 + t_3x_3 \equiv 0.$

REFERENCE

1. Bellman, R., Introduction to Matrix Analysis, McGraw-Hill Book Company, Inc., New York, 1960.